DaimlerChrysler AG

Vehicle security system

The vehicle relates to a vehicle security system and a method for operating this vehicle security system according to the preamble of Patent Claims 1 and 6.

In vehicle security systems in the form of what are referred to as keyless or "keyless-go" systems, authentication, i.e. checking of authorization, is carried out using portable, action-free authentication elements in the action range of a wirefree communications channel. Action range is understood here to be the range in which the authentication element must be located for a triggered access authentication checking process also to be actually carried out.

DE 44 09 167 C1 discloses using, in such a keyless-go system, a distance detection device which operates, for example, on the basis of UHF or ultrasonic signals or in the manner of a metal detector and measures the distance between an authentication element and the associated vehicle. After the reception of an interrogation code signal which is emitted by a transmitter unit which is arranged at the vehicle when a triggering means is actuated, the authentication element emits a response code signal only if the distance detection device determines that the distance between the authentication element and the vehicle is not greater than a predefinable maximum distance.

Furthermore, DE 195 42 441 C2 discloses various vehicle-mounted antenna units of access authorization communications channels and/or driving authorization communications channels for vehicle security systems with action-free authentication elements in the form of portable transponders which can be carried by a person,

with possible positioning processes of the antennas and their resulting action range being specified. Depending on which antenna or antennas emit(s) an interrogation code signal and which antenna receives a response code signal from the transponder with which intensity it is possible to locate the transponder and where necessary also follow it as it moves.

Finally, DE 198 39 355 C1 discloses a vehicle security system having an access control device. The access control device comprises one or more action-free authentication elements which can be carried by a user, a vehicle-mounted access control component, a wirefree access authorization communications channel for access-authorization-checking processes and a triggering element which can be addressed by a user in order to request the generation of a securing or releasing access control signal for at least one vehicle lock element. The access control component triggers an access-authorization-checking process in response to such a request and said process is carried out successfully only if the respective authentication element is located in the predefined action range of this communications channel. In addition, authentication element locating means are provided for determining whether an authentication element is located on the outside of a vehicle in the action range of the communications channel when an access-authorization-checking communications process is triggered. At least some of the possible securing or releasing access control signals are then generated as a function of whether a valid authentication element is determined on the outside of the vehicle.

In such conventional keyless-go systems, in order to locate an authentication element, for example a key, chip card or the like, pulses are thus transmitted from different antennas from the vehicle to the

authentication element and back. These pulses may have different frequencies and different forms. By means of these pulses the authentication element or an authentication element locating means in the vehicle determines its position at the vehicle. However, if there are additionally interference transmitters present which transmit in the same frequency range, the position of the authentication element at the vehicle/ with respect to the vehicle may be evaluated incorrectly. For example, the authentication element could be located outside the vehicle but as a result of the interference transmitter a field strength is present which indicates that the authentication element must be located in the vehicle. This may result in malfunctions, in particular as a result of the incorrect evaluation as to whether the authentication element is inside or outside the vehicle. For example, locking may not be possible even though the authentication element is located outside the vehicle but as a result of the interference signal the authentication element is evaluated as being located inside the vehicle.

For this reason the object of the present invention is to develop a device of the generic type and a method of the generic type for determining the position of a key of a keyless-go system in such a way that irrespective of the presence of interference transmitters the position of the authentication element can be reliably determined at the vehicle.

According to the invention this object is achieved by means of a vehicle security system and a method for operating a vehicle security system having the features of Patent Claims 1 and 6.

In this way it is possible to improve the process of locating the authentication element, i.e. incorrect

interpretation of the location of the authentication element is prevented when an interference transmitter is present. As a result the delimitation between the inside and outside regions of the vehicle becomes more precise. Malfunctions as a result of incorrect interpretation of the position of the authentication element can thus be reliably prevented.

This and further objects, features and advantages of the present invention become apparent from the following description of a preferred exemplary embodiment in conjunction with the drawing, in which:

Fig. 1 shows a block circuit diagram of a vehicle security system according to the invention,

Fig. 2 shows a flowchart explaining the function of the vehicle security system according to Fig. 1, and

Fig. 3 is an illustration of an exemplary signal profile during the inventive determination of an interference field strength by means of empty measurement.

In a keyless-go system which is used for a vehicle security system and has the purpose of locating an authentication element, for example a key or a code card or chip card, pulses are generally transmitted from different antennas from the vehicle to the authentication element and back. The pulses may have different frequencies and shapes. By means of these pulses the authentication element determines at/with respect to the vehicle. Alternatively this may be done by an authentication element locating means in the vehicle.

The vehicle security system which is illustrated schematically in fig. 1 contains an access control device and an electronic immobilizer and is embodied as

a keyless-go system, i.e. one or more action-free authentication elements which can be carried by the user, one of which is presented by way of representation in fig. 1, and which can be used by the user to prove his authorization to enter the vehicle and start it. An independent code card or chip card may, for example, be used as the authentication element. Alternatively, a chip card or a functionally equivalent authentication element may be integrated into a mechanical or electronic key, if the intention is that the user will be enabled optionally also to enter or to lock the vehicle and/or to start the engine or shut it down in a customary fashion by means of such a key system. Other conventional types of authentication elements can also be used.

At the vehicle end the vehicle security system contains a control unit 2 which is common to an access control device and an electronic immobilizer, while alternatively it is also respectively possible to provide separate control units. An antenna unit 3 with a plurality of suitably configured antennas which are positioned at the vehicle is connected to the control unit 2 and the control unit 2 communicates with the respective authentication element 1 via said antennas in order to carry out authentication processes. This communication is carried out for communications processes which relate to the vehicle access by means of a wirefree access authorization communications channel 4 and for communications processes which relate to the electronic immobilizer by means of a wirefree driving authorization communications channel 5. The two communications channels 4, 5 are preferably combined to form one, common communications channel. In all cases, the authentication element 1 is configured in such a way that it is capable of communicating with the control unit 2 to test both the access authorization and the driving authorization, which may entail a

respectively identical authentication process when there is a common communications channel. The communications channel or channels may be, for example, a frequency band around 433 MHz, also around 315 MHz for the USA, or alternatively around 125 kHz. The frequency band in the case of 433 MHz permits typical ranges in the region from approximately 1 km to approximately 30 m to be implemented cost-effectively. When the frequency band around 125 kHz is used, the range can be comparatively satisfactorily set by means of the exponentially dropping magnetic field.

The authentication element 1 preferably communicates bidirectionally with the vehicle-mounted system component over the communications channels 4, 5 and is preferably embodied without batteries, while it draws the required transmission energy from the field irradiated by the vehicle-mounted antenna unit 3. In applications in which this field which is irradiated at the vehicle end is too weak to supply energy to the authentication element 1 1, even at a distance of approximately 1 m, the authentication elements 1 are equipped with batteries in order to achieve a sufficiently large range. When the battery is empty the authentication element 1 can then be moved sufficiently close to the vehicle and thus be supplied with external energy.

Furthermore, a triggering unit 6 comprising a plurality of suitable triggering elements which can be addressed by the user and with which the user can request a desired control measure of the access control device or of the electronic immobilizer is connected to the control unit 2. In response to such a request, the control unit 2 firstly triggers an authentication process with which the authorization of the requesting user is checked. In order to carry out this authentication process successfully it is necessary for

at least one authentication element 1 which provides authorization for this vehicle to be located in the action range of the communications channel or channels 4, 5, i.e. within the action range or capture range of one or more antennas of the antenna unit 3. For this purpose it is sufficient in the case of a keyless-go system for the user to carry the authentication element 1 on his person. The action range of the access authorization communications channel 4 and that of the driving authorization communications channel 5 are respectively suitably selected for this purpose, in particular by suitable shaping and arrangement of the various antennas of the antenna unit 3.

The control unit 2 actuates both a closing unit 7 with a plurality of vehicle lock elements, in particular in each case a lock element for the vehicle doors and for a tailgate, and also an immobilizer unit 8 which contains, in a conventional way, suitable actuating elements for releasing or blocking an engine start, such as corresponding, actuatable switching elements for switching the ignition on and off and/or for starting the engine. Depending on whether a control measure for the access control device or the electronic immobilizer has been requested by the user by means of the triggering unit 6, the control unit 2 actuates the lock unit 7 or the immobilizer unit 8 as desired when the authentication process proceeds successfully. The lock unit 7 may be formed here in particular by a conventional central locking system which is switched by the securing or releasing access control signal of the control unit 2 into its locked or released state. Furthermore, it is possible to provide for the lock element for the tailgate to be capable of being actuated separately in order to be able to open it separately without releasing the vehicle doors.

Furthermore, authentication element locating means 21

which are implemented by means of hardware or software are provided in the control unit 2 and can be used to determine whether, when an access-authorization-checking communications process is triggered, an authorizing authentication element 1 is located on the outside of the vehicle in the action range of the access authorization communications channel 4. Here, the precise implementation of these authentication locating means 12 depends on the position of the action range of the access authorization communications channel 4, which action range corresponds to the combination of the action ranges of all the associated individual antennas, in particular on whether or not this action range also extends significantly into the inside of the vehicle, as explained below. The control unit 2 also performs the control measure which is requested by the user and relates to the vehicle access as a function of whether the authentication element locating means 21 have determined that an authorizing authentication element 1 which is located in the action range of the access authorization communications channel 4 and therefore results in a successful authentication process is located on the outside of the vehicle and not for example in the interior of the vehicle. For this purpose, a field strength of the signal in response to the access authorization communications channel 4 is determined and when a specific threshold value is exceeded the authentication element 1 is assessed as being located in the interior of the vehicle, i.e. the passenger compartment or trunk.

In order to prevent incorrect assessment of the position of the authentication element 1, in the interior of the vehicle or on the outside of the vehicle, by interference transmitters 6, as a result of which incorrect assessment opening takes place incorrectly or locking is incorrectly prevented,

according to the invention a device for performing empty measurement 9 (also shown in fig. 1) is additionally embodied in the authentication element 1.

In the exemplary embodiment according to the invention, the device for performing empty measurement 9 is designed to prevent incorrect assessments of the position of the authentication element 1 with respect to the vehicle owing to a field strength which is generated by at least one interference transmitter in the same frequency range. The device for performing empty measurement 9 measures an applied field strength at the useful frequency of the authentication element 1 at a time at which the vehicle does not emit any field, i.e. a signal is not transmitted from the vehicle on the access authorization communications channel 4. The field strength which is measured at this time corresponds to an interference field strength which is generated by one or more interference transmitters which happen to be present, i.e. to an interference level which has an adverse effect on the communication between the authentication element 1 and the vehicle on the access authorization communications channel 4. The interference field strength which is measured by the device for performing empty measurement 9 is subsequently used to evaluate the field strength of pulses from the vehicle which is measured in the "normal operating mode" and by means of which the position of the authentication element 1 with respect to the vehicle is determined. Depending on the size of the interference field strength which is determined by the device for performing empty measurement 9, the decision threshold value for distinguishing a position of an authentication element 1 on the outside of the vehicle or in the interior of the vehicle (in the case of low or medium-sized interference field strengths is adapted to a level at which an unambiguous detection is still possible, in response to which this adapted

decision threshold value is transmitted to the control unit with the authentication element locating means 21, or the field strengths (in the case of high to very high interference field strengths) which are determined during subsequent communication which is subject to such interference are rejected, i.e. when an interrogation signal is subsequently received from the vehicle a response signal is not transmitted on the access authorization communications channel 4.

The function of the vehicle security system according to the invention which is shown in fig. 1 will be explained further below with reference to the flowchart in fig. 2. In the keyless-go system contained in the vehicle security system, the control unit 2 emits pulses, which are intended for the authentication element 1 of the keyless-go system (step S1), over the access authorization communications channel 4 by means of the antenna unit 3 with various antennas arranged at various positions at the vehicle or in the vehicle. As soon as the authentication element 1 of the keyless-go system is located in the range of these pulses, the authentication element 1 is "woken up", i.e. activated (step S2). After the activation, synchronization is carried out between the authentication element 1 and the vehicle in step S3 in response to such a pulse from the vehicle. On the basis of this synchronization a device for performing empty measurement of the authentication element 1 knows the predetermined intervals at which the vehicle will emit further pulses.

After the synchronization, the device for performing empty measurement 9 carries out an empty measurement in step S4 by an interference level of one or more interference transmitters which happen to be present being determined in the same frequency range in a time period or at a time in or at which the vehicle does not

emit any pulses. Owing to the determined interference level, i.e. the determined interference field strength, either a signal from the vehicle to the authentication element 1 which is measured directly before or after is rejected in step S5 as a function of the determined level of the interference field strength if a predetermined threshold value for the interference level or the interference field strength is exceeded since then reliable detection is no longer possible, i.e. a response signal is not transmitted to the control unit 2 over the access authorization communications channel 4 by means of the authentication element locating means 21 in the vehicle, or a new threshold value, adapted to the interference field strength, for distinguishing between an authentication element 1 in the vehicle or on the outside of the vehicle is determined by the device for performing empty measurement and is transmitted over the access authorization communications channel 4 to the control unit 2 by means of the authentication element locating means 21 so that it can be taken into account during subsequent position-determining processes. If a response signal is not transmitted to the vehicle owing to the excessively large interference level, correct detection is possibly not possible until the authentication element 1 is located nearer to the vehicle, and if not in such a case it is necessary to have recourse to a conventional key. However, this ensures fault-free functioning of the vehicle security system so that no unintentional locking or release processes occur.

Finally, Fig. 3 shows, by way of example, both the transmission signal profile of the pulses from the vehicle and the transmission signal profile of the authentication element 1 including the empty measurements. In this illustration, possible alternative or additional times for empty measurements

are illustrated by dashed lines. It is generally to be noted that an empty measurement can be carried out at any time in the transmission protocol only as long as it is ensured that the vehicle does not emit any pulses at this time so that only one interference level is sensed.

To summarize, the invention relates to a vehicle security system in the form of a keyless-go system and an operating method for it. In the vehicle security system, incorrect detection of a position of an authentication element 1 inside or outside the vehicle by authentication element locating means 21 in a vehicle-mounted access control component owing to at least one interference transmitter 10 which is present in the surroundings of the vehicle and/or of the authentication element 1 is avoided by using a device for performing empty measurement 9 in the authentication element 1. To do this, the device for performing empty measurement 9 performs a measurement in time periods in which the vehicle-mounted access control component 2 does not emit any pulses to the authentication element 1, by means of which measurement the interference level caused by the at least one interference transmitter 10 is determined. Depending on whether this determined interference level exceeds or drops below a predetermined threshold value, either the device for performing empty measurement 9 transmits, to the vehicle-mounted access control component 2, an adapted threshold value for a decision as to whether an authentication element 1 is located in the vehicle or on the outside of the vehicle, or said device does not respond to subsequent pulse from the vehicle-mounted access control component 2.